AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions of claims in the application:

Listing of Claims:

1. (Currently Amended) A method for registering a first device with a second device, comprising the steps of:

initiating communication between the first device and the second device over a first communication channel ~~using a first communication method~~ by engaging a trigger at the first device and detecting at the second device that the trigger at the first device has been engaged;

upon initiation of communication between the first device and the second device, deriving a commitment value at the first device from a registration nonce value known to the first device and communicating the commitment value from the first device to the second device;

communicating information from the second device to the first device for use in generating a secret;

communicating a registration nonce value from the first device to the second device in response to the information communicated from the second device;

at the second device, attempting to derive the commitment value from the registration nonce value communicated from the first device;

if the commitment value is successfully derived by the second device, generating a first secret known to the first device and a second secret known to the second device using communications between the first device and the second device over the first communication channel ~~using the first communication method~~;

from the first device, producing first information derived from the first secret;

from the second device, producing second information derived from the second secret;

using a communication channel other than the first communication channel ~~and a communication method other than the first communication method~~, comparing the first information and the second information in a manner sufficient to assure a third party that the first secret and the second secret are the same; and

enabling the first and second device to use the first and second secrets upon the third party being assured that the first secret and the second secret are the same.

2. (Original) The method of claim 1 wherein the first device and the second device generate the first and second secrets using Diffie-Hellman key exchange.

3. (Original) The method of claim 1 wherein:
the first information is derived from a hash of the first secret; and
the second information is derived from a hash of the second secret.

4. (Original) The method of claim 1 wherein the first information comprises a credential.

5. (Currently Amended) A method for registering a first device with a second device, comprising the steps of:

(a) engaging a trigger coupled to the first device, wherein the trigger is ~~comprising one or more of~~ a switch or a button;

(b) detecting at the second device that the trigger coupled to the first device has been engaged;

(c) after step (b), communicating a commitment value from the first device to the second device over a first communication channel ~~using a first communication method~~, wherein said commitment value is ~~comprising information~~ derived from a security value known to the first device;

(d) communicating from the second device to the first device over the first communication channel, information for use in generating a first secret;

(e) after step (d), communicating [[the]] a security value from the first device to the second device;

(f) at the second device, attempting to derive the commitment value communicated to the second device at step [[(a)]] (c) from the security value communicated to the second device at step [[(c)]] (e) and terminating registration if the commitment value is not correctly derived from the security value;

(g) generating the first secret at the first device and a second secret at the second device;

(h) from the first device, on a communication channel other than the first communication channel ~~and using a communication method other than the first communication method~~, validating first verification information related to the first secret;

(i) from the second device, on a communication channel other than the first communication channel ~~and using a communication method other than the first communication method~~, validating second verification information related to the second secret; and

(j) enabling the first and second devices to use the first and second secrets upon a third party being assured that the first secret and the second secret are the same.

6. (Currently Amended) The method of claim 5 wherein the commitment value is a hash of the security value.

7. (Original) The method of claim 5 wherein the first verification information is a hash value derived from the first secret and the security value.

8. (Original) The method of claim 7 wherein the first verification information is a hash value derived from a catenation of the first secret with the security value.

9. (Currently Amended) The method of claim 5 wherein the length of the first verification information is shorter than a length needed to provide an identical level of security in a method that does not utilize ~~said commitment~~ a commitment value.

10. (Original) The method of claim 5 wherein the first verification information comprise a credential.

11. (Currently Amended) A device capable of registering with an other device, comprising:

a trigger coupled to the device, the trigger comprising a switch or a button;

an interface to a first communication channel associated with a first communication method;

an interface to a second communication channel associated with a communication method other than the first communication method; and

a registration process that (1) initiates communication with the other device over the first communication channel upon engagement of the trigger coupled to the device and acknowledgement at the other device that the trigger has been engaged, (2) receives a hash of a security value from the other device using the first communication channel, (3) receives a security value from the other device using the first communication channel and terminates registration if a generated hash of the security value received from the other device differs from the hash received at step (2), (4) generates a first secret that is to-be-shared with the other device using the first communication channel, [[(3)]] (5) validates on the second communication channel verification information derived from the to-be-shared secret, and [[(4)]] (6) is enabled to use the to-be-shared secret upon receipt of an indication that a third party is assured that the first secret is shared with the other device.

12. (Original) The device of claim 11 wherein the device generates the first secret using a Diffie-Hellman key exchange.

13. (Original) The device of claim 11 wherein the verification information is derived from a hash of the first secret.

14. (Original) The device of claim 11 wherein the verification information comprises a credential.

15. (Currently Amended) A device capable of registering with an other device, comprising:

a trigger coupled to the device;

an interface to a first communication channel associated with a first communication method;

an interface to a second communication channel associated with a communication method other than the first communication method; and

a registration process that (1) initiates communication with the other device over the first communication channel upon engagement of the trigger coupled to the device, (2) receives, on

the first communication channel, a commitment value derived from a security value; (3) produces, on the first communication channel, information for use in generating a shared secret; (4) after step (3), ~~communicates~~ receives [[the]] a security value on the first communication channel; (5) attempts to derive the commitment value received at step (2) from the security value received at step (4) and, if the commitment value is not successfully derived from the security value, terminates the registration process; [[(5)]] (6) generates a first secret to-be-shared with the other device, [[(6)]] (7) communicates on the second communication channel verification information related to the first secret, and [[(7)]] (8) is enabled to use the first secret upon receipt of an indication that a third party is assured that the first secret is [[hared]] shared with the other device.

16. (Currently Amended) The device of claim 15 wherein the commitment value is a hash of the security value.

17. (Original) The device of claim 15 wherein the verification information is a hash value derived from the first secret and the security value.

18. (Original) The device of claim 17 wherein the verification information is a hash value derived from the catenation of the first secret with the security value.

19. (Currently Amended) The device of claim 15 wherein the length of the verification information is shorter than a length needed to provide an identical level of security in a method that does not utilize ~~said commitment~~ a commitment value.

20. (Original) The method of claim 15 wherein the verification information is a credential.

21. (Currently Amended) A server capable of registering a device to a network, comprising:

an interface to a first communication channel associated with a first communication method;

an interface to a second communication channel associated with a communication method other than the first communication method; and

a registration process that (1) derives a commitment value from a registration nonce by computing a hash of the registration nonce and communicates the commitment value to the device on the first communication channel ~~generates a first secret that is to be shared with the device using the first communication channel~~ upon detecting that a trigger coupled to the device has been engaged; (2) after step (1), communicates a registration nonce to the device on the first communication channel; (3) upon determining that the device has successfully derived the commitment value from the registration nonce, generates a first secret that is to be shared with the device using the first communication channel; (4) validates verification information derived from the first secret on the second communication channel[[,]]; and [[(3)]] (5) enables the network to use the first secret upon receipt of an indication that a third party is assured that the ~~to be shared~~ first secret is shared with the device.

22. (Original) The server of claim 21 wherein the server generates the first secret using Diffie-Hellman key exchange.

23. (Currently Amended) The server of claim 21 wherein the verification information is derived from a hash of the first secret.

24. (Original) The server of claim 21 wherein the verification information comprises a credential.

25. (Currently Amended) A server capable of registering a device to a network, comprising:

an interface to a first communication channel associated with a first communication method;

an interface to a second communication channel associated with a communication method other than the first communication method; and

a registration process that (1) determines that the registration process has been initiated at the device by detecting that a trigger physically coupled to the device has been engaged; (2) after step (1), communicates to the device over the first communication channel a commitment comprising information derived from a security value ~~upon detecting that the registration process has been initiated at the device by engaging a trigger coupled to the device;~~ [[(2)]] (3)

communicates to the device over the first communication channel information for use in generating a shared secret; [[(3)]] (4) after step [[(2)]] (3), communicates the security value to the device over the first communication channel and terminates the registration process upon an indication from the device that the device has unsuccessfully attempted to derive the commitment communicated at step (2) from the security value; [[(4)]] (5) generates a first secret to-be-shared with the device; [[(5)]] (6) communicates over the second communication channel verification information related to the secret; and [[(6)]] (7) enables the network to use the first secret upon receipt of an indication that a third party is assured that the first secret is shared with the device.

26. (Currently Amended) The server of claim 25 wherein the commitment is a hash of the security value.

27. (Original) The server of claim 25 wherein the verification information is a hash value derived from the secret and the security value.

28. (Original) The server of claim 27 wherein the verification information is a hash value derived from the catenation of the first secret with the security value.

29. (Currently Amended) The server of claim 25 wherein the length of the verification information is shorter that a length needed to provide an identical level of security in a method that does not utilize [[said]] a commitment.

30. (Original) The method of claim 25, wherein the verification information comprises a credential.